(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101471942 B
(45)授权公告日 2012.12.05

(21)申请号 200810175269.8
(22)申请日 2008.11.10
(30)优先权数据
2007-334998 2007.12.26 JP
(73)专利权人 冲电气工业株式会社
地址 日本东京都
(72)发明人 新谷义弘
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 雒运朴 李伟
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
WO 2006/095895 A1,2006.09.14, 全文.
CN 1527173 A,2004.09.08, 全文.
审查员 高菲

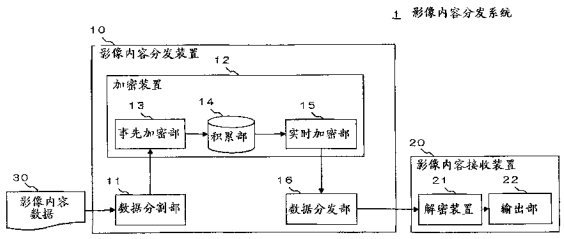
权利要求书 2 页 说明书 11 页 附图 17 页

(54)发明名称

加密装置、解密装置、数据提供装置、数据接收装置

(57)摘要

本发明提供一种将数据分发至数据接收装置的数据提供系统，其减轻数据分发时的加密导致的处理负荷，并且防止对分发对象的数据的非法阅览。本发明涉及一种将分割一个数据而得到的多个分割数据的每个进行加密并发送至数据接收装置的数据提供系统和具有数据接收装置的数据提供系统。并且其特征在于，在数据提供系统所具有的加密装置中，具有对多个分割数据中一部分分割数据进行加密的单元、保持被加密的分割数据和未被加密的分割数据的单元、在将数据提供系统保持的分割数据的每个向数据接收装置发送时将未被加密的分割数据加密并使数据提供系统发送的单元。



CN 101471942 B

1. 一种加密装置，该加密装置是数据提供装置所具有的，该数据提供装置将分割一个数据而得到的多个分割数据的每个加密并向数据接收装置发送，该加密装置的特征在于，

具有：第一加密单元，只对上述多个分割数据中的判断为待加密的分割数据进行加密；

保持单元，保持由上述第一加密单元加密后的分割数据和上述多个分割数据中未由上述第一加密单元加密的分割数据；

以及第二加密单元，在上述数据提供装置将由上述保持单元保持的分割数据的每个向上述数据接收装置发送时，对基于加密状态判断为未加密的分割数据进行加密后使上述数据提供装置发送。

2. 根据权利要求 1 所述的加密装置，其特征在于，

上述多个分割数据的每个具有表示该分割数据的加密状态的加密状态信息；

上述第一加密单元，在加密分割数据时，在该分割数据的加密状态信息中设定表示已由上述第一加密单元加密这一情况的信息；

上述第二加密单元基于上述保持单元保持的分割数据的加密状态信息的内容，判定该分割数据是否已被加密，在对上述保持单元保持的分割数据中未被加密的分割数据进行加密时，对该分割数据的加密状态信息设定表示已由上述第二加密单元加密这一情况的信息。

3. 根据权利要求 1 或 2 所述的加密装置，其特征在于，上述第一加密单元和上述第二加密单元中加密分割数据的加密条件不同。

4. 根据权利要求 1 所述的加密装置，其特征在于，

上述多个分割数据的每个具有表示该分割数据的加密状态的加密状态信息；

上述第一加密单元在加密分割数据时，对该分割数据的加密状态信息设定表示已加密这一情况的信息；

上述第二加密单元基于上述保持单元保持的分割数据的加密状态信息的内容，判定该分割数据是否已被加密。

5. 一种加密方法，其特征在于，该加密方法是数据提供装置所具有的加密装置所执行的方法，该数据提供装置将分割一个数据而得到的多个分割数据的每个加密并向数据接收装置发送，该加密方法包括：

第一加密步骤，只对上述多个分割数据中的判断为待加密的分割数据进行加密；

保持步骤，保持在上述第一加密步骤中加密后的分割数据和上述多个分割数据中未在上述第一加密步骤中加密的分割数据；

以及第二加密步骤，在上述数据提供装置将在上述保持步骤中保持的分割数据的每个向上述数据接收装置发送时，对基于加密条件判断为未加密的分割数据进行加密后使上述数据提供装置发送。

6. 一种数据提供装置，将分割一个数据而得到的多个分割数据的每个加密并向数据接收装置发送，其特征在于，包括权利要求 1 所述的对上述多个分割数据的每个进行加密的加密装置。

7. 一种解密装置，是接收数据提供装置提供的分割数据并进行解密的数据接收装置所具有的解密装置，且该数据提供装置是权利要求 6 所述的数据提供装置，其特征在于，

具有解密单元，用以适用与上述数据提供装置提供的分割数据的每个所具有的、表示该分割数据的加密状态的加密状态信息对应的解密条件，对上述数据提供装置提供的分割数据的每个进行解密。

8. 一种解密方法，其特征在于，是数据接收装置所具有的解密装置所执行的方法，该解密装置接收数据提供装置提供的分割数据并进行解密，该数据提供装置将分割一个数据而得到的多个分割数据的每个加密并向数据接收装置发送，该解密方法包括：

解密步骤，用以适用与上述数据提供装置提供的分割数据的每个所具有的、表示该分割数据的加密状态的加密状态信息对应的解密条件，对上述数据提供装置提供的分割数据的每个进行解密。

9. 一种数据接收装置，是接收数据提供装置提供的多个分割数据并进行解密的数据接收装置，且该数据提供装置将分割一个数据而得到的上述多个分割数据的每个加密并发送，其特征在于，

包括权利要求 7 所述的对上述多个分割数据的每个进行解密的解密装置。

10. 一种数据提供系统，是具有数据提供装置和数据接收装置的数据提供系统，且该数据提供装置将分割一个数据而得到的多个分割数据的每个加密并向数据接收装置发送，该数据接收装置从上述数据提供装置接收分割数据并进行解密，其特征在于，

作为上述数据提供装置，包括权利要求 6 所述的数据提供装置。

加密装置、解密装置、数据提供装置、数据接收装置

技术领域

[0001] 本发明涉及加密装置、加密程序、解密装置、解密程序、数据提供装置、数据接收装置及数据提供系统，例如可适用于分发影像内容的系统。

背景技术

[0002] 当前，在因特网上分发电影等影像内容的网络服务日益盛行。一般地，为了进行著作权等的保护和避免非法流通，将影像内容加密，从而使合法权利者之外的人无法看到。

[0003] 以往，对于分发至因特网的影像内容，例如专利文献 1 中记载的内容分发系统那样进行事先加密或在分发时实时加密中的任意一者。

[0004] [专利文献 1] 日本特开 2007-13765 号

[0005] 但是，事先加密虽然没有分发时的处理负荷，但一旦密码被破坏，必须再次进行加密，安全强度低于实时加密，而且，还必须进行适当的解密密钥的保管。此外，实时加密虽然在分发时的处理负荷较高，但即使密码被破坏，由于每次都进行变更，所以对安全强度的影响较少。此外也无须进行解密密钥的保管，管理比较容易。但是，能了解影像内容的积累方法的相关人员容易非法取得影像内容。虽然也开发了实施事先加密，在分发时将其解密后再次进行加密来进行分发的技术，但存在着处理负荷高的缺点。

发明内容

[0006] 因此，需要一种能够减轻数据分发时的加密导致的处理负荷，并且能够防止对分发对象的数据的非法阅览的加密装置、加密程序、解密装置、解密程序、数据提供装置、数据接收装置及数据提供系统。

[0007] 本发明之一的加密装置，(1) 是将分割一个数据而得到的多个分割数据的每个加密并向数据接收装置发送的数据提供装置所具有的加密装置，其特征在于，具有 :(2) 第一加密单元，只对上述多个分割数据中的一部分分割数据进行加密 ;(3) 保持单元，保持由上述第一加密单元加密后的分割数据和上述多个分割数据中未由上述第一加密单元加密的分割数据 ;以及 (4) 第二加密单元，在上述数据提供装置将由上述保持单元保持的分割数据的每个向上述数据接收装置发送时，对未加密的分割数据进行加密后使上述数据提供装置发送。

[0008] 本发明之二的加密程序，其特征在于，(1) 是使加密装置中所搭载的计算机作为如下单元而发挥功能，且该加密装置是将分割一个数据而得到的多个分割数据的每个加密并向数据接收装置发送的数据提供装置所具有的 :(2) 第一加密单元，只对上述多个分割数据中的一部分分割数据进行加密 ;(3) 保持单元，保持由上述第一加密单元加密后的分割数据和上述多个分割数据中未由上述第一加密单元加密的分割数据 ;以及 (4) 第二加密单元，在上述数据提供装置将由上述保持单元保持的分割数据的每个向上述数据接收装置发送时，对未加密的分割数据进行加密后使上述数据提供装置发送。

[0009] 本发明之三的数据提供装置，(1) 将分割一个数据而得到的多个分割数据的每个

加密并向数据接收装置发送，其特征在于，(2) 使用本发明之一的加密装置对上述多个分割数据的每个进行加密。

[0010] 本发明之四的解密装置，(1) 是接收数据提供装置提供的分割数据并进行解密的数据接收装置所具有的解密装置，且该数据提供装置将分割一个数据而得到的多个分割数据的每个加密并发送，其特征在于，具有 (2) 解密单元，用以适用与上述数据提供装置提供的分割数据的每个所具有的、表示该分割数据的加密状态的加密状态信息对应的解密条件，对上述数据提供装置提供的分割数据的每个进行解密。

[0011] 本发明之五的解密程序，其特征在于，(1) 是使解密装置中所搭载的计算机作为如下单元而发挥功能，且该解密装置是接收数据提供装置提供的分割数据并进行解密的数据接收装置所具有的解密装置，且该数据提供装置将分割一个数据而得到的多个分割数据的每个加密并发送：(2) 解密单元，用以适用与上述数据提供装置提供的分割数据的每个所具有的、表示该分割数据的加密状态的加密状态信息对应的解密条件，对上述数据提供装置提供的分割数据的每个进行解密。

[0012] 本发明之六的数据接收装置，(1) 是接收数据提供装置提供的上述多个分割数据并进行解密的数据接收装置，且该数据提供装置将分割一个数据而得到的多个分割数据的每个加密并发送，其特征在于，(2) 使用本发明之四的解密装置，对上述多个分割数据的每个进行解密。

[0013] 本发明之七的数据提供系统，(1) 是具有数据提供装置和数据接收装置的数据提供系统，且该数据提供装置将分割一个数据而得到的多个分割数据的每个加密并向数据接收装置发送，该数据接收装置从上述数据提供装置接收分割数据并进行解密，其特征在于，(2) 作为上述数据提供装置，适用本发明之三的数据提供装置。

[0014] 根据本发明，在将数据分发至数据接收装置的数据提供系统中，能够减轻数据分发时的加密导致的处理负荷，并且能够防止对分发对象的数据的非法阅览。

附图说明

[0015] 图 1 是表示第一实施方式涉及的实施方式的影像内容分发系统的整体构成的方框图。

[0016] 图 2 是表示第一实施方式涉及的分割后的影像内容数据的例 (TS 数据包) 的构成的说明图。

[0017] 图 3 是表示第一实施方式涉及的事先加密部的内部构成的方框图。

[0018] 图 4 是表示第一实施方式涉及的加密方式的例的说明图。

[0019] 图 5 是表示第一实施方式涉及的实时加密部的内部构成的方框图。

[0020] 图 6 是表示第一实施方式涉及的解密装置的内部构成的方框图。

[0021] 图 7 是表示第一实施方式涉及的影像内容分发系统中进行数据分发的动作的整体的流程图。

[0022] 图 8 是表示第一实施方式涉及的事先加密部的动作的详细情况的流程图。

[0023] 图 9 是表示第一实施方式涉及的实时加密部的动作的详细情况的流程图。

[0024] 图 10 是表示第一实施方式涉及的解密装置的动作的详细情况的流程图。

[0025] 图 11 是表示第二实施方式涉及的影像内容分发系统的整体构成的方框图。

[0026] 图 12 是表示第二实施方式涉及的事先加密部的内部构成的方框图。

[0027] 图 13 是表示第二实施方式涉及的实时加密部的内部构成的方框图。

[0028] 图 14 是表示第二实施方式涉及的解密部的内部构成的方框图。

[0029] 图 15 是表示第二实施方式涉及的影像内容分发系统中进行数据分发的动作的整体的流程图。

[0030] 图 16 是表示第二实施方式涉及的事先加密部的动作的详细情况的流程图。

[0031] 图 17 是表示第二实施方式涉及的实时加密部的动作的详细情况的流程图。

[0032] 图 18 是表示第二实施方式涉及的解密装置的动作的详细情况的流程图。

[0033] 图中 :1- 影像内容分发系统 ;10- 影像内容分发装置 ;11- 数据分割部 ;12- 加密装置 ;13- 事先加密部 ;131- 数据读入处理部 ;132- 加密判定部 ;133- 加密部 ;14- 数据积累部 ;15- 实时加密部 ;151- 数据读入处理部 ;152- 加密判定部 ;153- 加密部 ;154- 加密标志设定部 ;16- 数据分发部 ;20- 影像内容接收装置 ;21- 解密装置 ;211- 数据接收部 ;212- 解密处理部 ;30- 影像内容数据。

具体实施方式

[0034] (A) 第一实施方式

[0035] 下面参照附图详细描述根据本发明的加密装置、加密程序、解密装置、解密程序、数据提供装置、数据接收装置及数据提供系统的第一实施方式。另外，该实施方式的数据提供装置、数据接收装置及数据提供系统为影像内容分发装置、影像内容接收装置及影像内容提供系统。

[0036] (A-1) 第一实施方式的构成

[0037] 图 1 是表示该实施方式的影像内容分发系统 1 的整体构成的方框图。

[0038] 影像内容分发系统 1 具有影像内容分发装置 10 及影像内容接收装置 20，例如，利用影像内容分发装置 10 对影像内容数据 30 等分发对象数据加密后分发至影像内容接收装置 20。另外，在图 1 中为了简化说明，影像内容分发装置 10 及影像内容接收装置 20 分别为一个，但是也可以分别有多个。

[0039] 影像内容分发装置 10 将影像内容数据 30 分割为多个数据，对分割后的数据的每个进行加密后分发至影像内容接收装置 20，具有数据分割部 11、加密装置 12 和数据分发部 16。影像内容分发装置 10 是在具有 CPU、ROM、RAM、EEPROM、硬盘等程序执行构成及用于与其他通信装置进行通信的接口的装置（不限于一台，也可以构成为可以将多台进行分布式处理）上，通过安装实施方式的加密程序等构造而成，可以如上述图 1 那样进行功能性的表示。

[0040] 数据分割部 11 得到影像内容数据 30 后分割影像内容数据并将分割后的数据提供给加密装置 12。作为取入影像内容数据 30 的单元，也可以将数据分割部 11 构成为，从存储介质和装置内置的存储装置进行取入，或者通过从外部装置下载进行取入，对取入方法不作限定。

[0041] 数据分割部 11 也可以在分割影像内容数据 30 时，生成将分割后的数据的每个放入规定格式的数据包中而得到的数据。在该实施方式中，作为例子，设成数据分割部 11 生成 MPEG(Moving Picture Experts Group) 中的 TS(Transport Stream) 格式的数据包（以

下称为“TS数据包”),而进行说明。另外,数据分割部11生成的数据包也可以是PS(Program Stream)形式等的可变长的数据包,对其形式不作限定。

[0042] 图2是表示TS数据包的构成的说明图。TS数据包由188字节构成一个数据包。

[0043] 加密装置12将数据分割部11提供的TS数据包的每个加密后提供给数据分发部16,具有事先加密部13、数据积累部14及实时加密部15。

[0044] 加密装置12是在具有CPU、ROM、RAM、EEPROM、硬盘等程序执行构成及用于与其他通信装置进行通信的接口的装置(不限于一台,也可以构成为可以将多台进行分布式处理)上,通过安装实施方式的加密程序等构造而成,可以如上述图1那样进行功能性的表示。

[0045] 加密装置12将多个TS数据包的一部分预先加密,在实际进行数据分发时,将事先未加密的TS数据包加密后提供给数据分发部16。

[0046] 图3是表示事先加密部13的内部构成的方框图。

[0047] 事先加密部13在对影像内容接收装置20进行数据分发之前,预先将影像内容数据30的一部分,即多个TS数据包中的一部分加密后提供给数据积累部14,具有数据读入处理部131、加密判定部132及加密处理部133。

[0048] 数据读入处理部131从数据分割部11读入TS数据包并提供给加密判定部132。

[0049] 加密判定部132从数据读入处理部131得到TS数据包后,判定是否事先加密该TS数据包,并将判定为要加密的TS数据包提供给加密处理部133,将判定为不进行加密的TS数据包提供给数据积累部14。

[0050] 加密判定部132基于规定的评价函数判定是否对TS数据包进行加密。例如,也可以根据该TS数据包的头信息的内容进行判定,也可以判定为对每隔一个等规定间隔的TS数据包进行加密,还可以根据该TS数据包的帧的种类进行判定,对判定方法不作限定。在该实施方式中,作为例子,将加密判定部132设为根据TS数据包的头信息的内容判定是否进行加密。

[0051] 如上述图2所示,TS数据包的头部分中具有两比特的表示加密的信息(Transport_scrambling_control,以下称为“加密标志”),使用方法可由用户任意定义。在该实施方式的加密判定部132中,作为例子,根据该加密标志的值判定是否进行加密。例如,此处,加密标志的值为“01”时则进行加密。这样,加密标志在影像内容分发系统1中作为表示该TS数据包的加密状态的信息被参照和登记。

[0052] 在根据加密标志的值判定是否进行加密的情况下,也可以当在上述数据分割部11中生成TS数据包时赋予任意的值。例如,也可以另外具有产生随机数的单元并根据该随机数进行赋予,也可以如“00、01、10、11、00、01、10、...”等巡回地赋予其值,还可以对每个规定间隔的TS数据包赋予“01”,对该赋予方法不作限定。

[0053] 加密处理部133将由加密判定部132提供的TS数据包加密后提供给数据积累部14。也可以在加密处理部133中,仅加密TS数据包的数据部分(上述图2中的Data_byte(净荷))。另外,加密处理部133中的加密形式也可以设成不参照紧邻的前一结果的方式。

[0054] 图4是表示加密方式的例子的说明图。

[0055] 例如,在该实施方式中,如图4所示,在加密每个TS数据包的数据时,也可

设成不参照紧邻的前一个 TS 数据包的加密结果而进行加密的方式，具体而言可适用 AES(Advanced Encryption Standard) 的方式。

[0056] 数据积累部 14 保持由事先加密部 13 提供的 TS 数据包，在向影像内容接收装置 20 分发数据时，将 TS 数据包提供给实时加密部 15。另外，在数据积累部 14 中，也可以与 TS 数据包一起组合保存加密密钥及解密密钥。此外，也可以将数据积累部 14 配置于加密装置 12 的外部，在每次数据分发时加密装置 12 进行读入，只要能够保持由事先加密部 13 进行部分加密的 TS 数据包，对该单元不作限定。

[0057] 图 5 是表示实时加密部 15 的内部构成的方框图。

[0058] 实时加密部 15 将由数据积累部 14 提供的 TS 数据包中的未被加密的 TS 数据包进行加密并提供给数据分发部 16，具有数据读入处理部 151、加密判定部 152、加密处理部 153 和加密标志设定部 154。

[0059] 数据读入处理部 151 从数据积累部 14 读入 TS 数据包并提供给加密判定部 152。

[0060] 加密判定部 152 在从数据读入处理部 151 得到 TS 数据包后，判定是否加密该 TS 数据包，并将判定为要进行加密的 TS 数据包提供给加密处理部 153，将判定为不进行加密的 TS 数据包提供给数据分发部 16。

[0061] 加密判定部 152 例如也可基于该 TS 数据包的加密标志的内容判定是否已加密。此处，例如加密标志为“01”时，如上所述，则为已由事先加密部 13 加密。

[0062] 加密处理部 153 将加密判定部 152 提供的 TS 数据包加密后提供给加密标志设定部 154。加密处理部 153 中的加密方式和加密密钥的内容等加密条件与加密处理部 133 相同。

[0063] 加密标志设定部 154 对由加密处理部 153 提供的 TS 数据包的头信息赋予表示已加密的情况的信息并提供给数据分发部 16。

[0064] 加密标志设定部 154，例如也可以对 TS 数据包的加密标志，设定与在加密处理部 133 中被加密的 TS 数据包不同的值。例如，在该实施方式的加密标志设定部 154 中，作为加密标志设定“10”的值。另外，在加密标志设定部 154 中，作为加密标志，也可以设定与在加密处理部 133 中被加密的 TS 数据包相同的值 (01)。

[0065] 数据分发部 16 将由实时加密部 15 提供的 TS 数据包向影像内容接收装置 20 发送。

[0066] 影像内容接收装置 20 从影像内容分发装置 10 接收被加密的 TS 数据包后，解密被加密的 TS 数据包并进行输出，具有解密装置 21 和输出部 22。

[0067] 图 6 是表示解密装置 21 的内部构成的方框图。

[0068] 解密装置 21 解密来自影像内容分发装置 10 的被加密的 TS 数据包，具有数据接收部 211、加密判定部 212 及解密处理部 213。

[0069] 解密装置 21 是在具有 CPU、ROM、RAM、EEPROM、硬盘等程序执行构成的装置（不限于一台，，也可以构成为可以将多台进行分布式处理）上，通过安装实施方式的解密程序等构造而成，可以如上述图 6 那样进行功能性的表示。

[0070] 数据接收部 211 读入从影像内容分发装置 10 提供给影像内容接收装置 20 的 TS 数据包，并提供给加密判定部 212。

[0071] 加密判定部 212 判定由数据接收部 211 提供的 TS 数据包是否已被加密，在判定为已被加密的情况下，将该 TS 数据包提供给解密处理部 213，在判定为未被加密的情况下按

原样提供给输出部。

[0072] 加密判定部 212 也可以根据 TS 数据包的加密标志的内容判定是否已被加密。如上所述，将由事先加密部 13 加密的 TS 数据包的加密标志设定为“01”，将由实时加密部 15 加密的 TS 数据包的加密标志设定为“10”，因此在加密标志为其中任意一者的值的情况下判定为已被加密。另外，即使是在事先加密部 13 和实时加密部 15 中，将被加密的 TS 数据包的加密标志例如设定为相同的“01”的构成的情况下，在由数据接收部 211 提供的 TS 数据包的加密标志为该值 (01) 时判定为已加密。

[0073] 解密处理部 213 进行由加密判定部 212 提供的 TS 数据包的解密并提供给输出部 22。关于在解密处理部 213 中解密所必需的解密密钥等信息，也可以预先登记，也可以在每次接收数据时从影像内容分发装置 10 或图 1 中省略图示的外部认证装置等读入并保持，对其取得方法不作限定。

[0074] 输出部 22 输出由解密装置 21 提供的 TS 数据包，例如，也可以对已解密的数据进行图像处理并将其向显示器等显示输出，也可以将其存储在内部或外部的盘装置等存储装置中，对其输出构成不作限定。

[0075] (A-2) 第一实施方式的动作

[0076] 接着，说明具有上述构成的第一实施方式的影像内容分发系统 1 的动作。

[0077] 图 7 是表示在影像内容分发系统 1 中将影像内容数据 30 从影像内容分发装置 10 向影像内容接收装置 20 进行数据分发的动作的整体的流程图。

[0078] 首先，影像内容分发装置 10 若被提供了影像内容数据 30，则在数据分割部 11 中分割并生成 TS 数据包，提供给加密装置 12(S110)。

[0079] 加密装置 12，若取得了 TS 数据包，则在事先加密部 13 中加密一部分 TS 数据包 (S120)。

[0080] 而且，在事先加密部 13 中被加密的 TS 数据包以及未被加密的 TS 数据包被积累到数据积累部 14 中 (S130)。

[0081] 接着，在进行数据分发时，积累在数据积累部 14 中的 TS 数据包被提供给实时加密部 15，将在上述步骤 S120 中未被加密的 TS 数据包加密后提供给数据分发部 16(S140)。

[0082] 在数据分发部 16 中，将由实时加密部 15 提供的 TS 数据包向影像内容接收装置 20 发送 (S150)。

[0083] 在影像内容接收装置 20 中，将由影像内容分发装置 10 提供的 TS 数据包利用解密装置 21 进行解密 (S160)。

[0084] 接着，说明上述步骤 S120 中的事先加密部 13 的动作的详细情况。

[0085] 图 8 是表示事先加密部 13 的动作的详细情况的流程图。

[0086] 在事先加密部 13 中，若从数据分割部 11 取得了 TS 数据包，则由数据读入处理部 131 读入并提供给加密判定部 132，在无要读入的 TS 数据包的情况下处理结束 (S121、S122)。

[0087] 而且，在加密判定部 132 中，利用规定的评价函数判定是否对该 TS 数据包进行加密，在判定为进行加密的情况下，将 TS 数据包提供给加密处理部 133，在判定为不进行加密的情况下，不进行加密而将 TS 数据包提供给数据积累部 14(S123、S125)。在步骤 S123 中，设成，在 TS 数据包的加密标志被设定为“01”时判定为进行加密。

[0088] 若将 TS 数据包从加密判定部 132 提供给加密处理部 133，则由加密处理部 133 对该 TS 数据包进行加密，并提供给数据积累部 14(S124、S125)。

[0089] 接着，说明上述步骤 S140 中的实时加密部 15 的详细情况。

[0090] 图 9 是表示上述步骤 S140 中的实时加密部 15 的动作的详细情况的流程图。

[0091] 在实时加密部 15 中，若从数据积累部 14 被提供了 TS 数据包，则由数据读入处理部 151 读入并提供给加密判定部 152，在无要读入的 TS 数据包的情况下处理结束 (S141、S142)。

[0092] 而且，在加密判定部 152 中，根据加密标志的内容判定该 TS 数据包是否已经被加密，将被判定为未被加密的 TS 数据包提供给加密处理部 153，将判定为已经被加密的 TS 数据包按原样提供给数据分发部 16(S143)。

[0093] 若将 TS 数据包从加密判定部 152 提供给加密处理部 153，则，由加密处理部 153 对该 TS 数据包加密并提供给加密标志设定部 154(S144)。

[0094] 若从加密处理部 153 提供了 TS 数据包，在加密标志设定部 154 中，对该 TS 数据包的加密标志设定为“10”，将设定了加密标志的 TS 数据包提供给数据分发部 16(S145、S146)。

[0095] 图 10 是表示上述步骤 S160 中的解密装置 21 的动作的详细情况的流程图。

[0096] 在解密装置 21 中，若从影像内容分发装置 10 提供了 TS 数据包，则由数据接收部 211 读入并提供给加密判定部 212，无要读入的 TS 数据包的情况下处理结束 (S161、S162)。

[0097] 接着，在加密判定部 212 中，根据加密标志的内容判定该 TS 数据包是否已经被加密，将判定为已被加密的 TS 数据包提供给解密处理部 213，将判定为未被加密的 TS 数据包按原样提供给输出部进行输出 (S163、S165)。在步骤 S163 中，设成，在 TS 数据包的加密标志已被设定为“01”或“10”时判定为已被加密。

[0098] 若将 TS 数据包从加密判定部 212 提供给解密处理部 213，则由解密处理部 213 对该 TS 数据包进行解密，并提供给输出部 22 进行输出 (S164、S165)。

[0099] (A-3) 第一实施方式的效果

[0100] 根据该实施方式，可取得以下效果。

[0101] 在加密装置 12 中，将根据作为分发对象的影像内容数据 30 生成的多个 TS 数据包的一部分预先由事先加密部 13 加密，在分发数据 (TS 数据包) 时，只将事先未被加密的 TS 数据包由实时加密部 15 加密。据此，实时加密部 15 无须加密所有 TS 数据包，因此可以降低分发影像内容数据 30 时加密所必须的处理量。

[0102] 此外，由于数据积累部 14 中所积累的数据中的一部分 TS 数据包已被加密，因此，即使非法取得了数据积累部 14 中积累的数据，也能够防止容易地重放 (阅览) 影像内容数据 30 的影像内容。

[0103] (B) 第二实施方式

[0104] 下面参照附图详细描述根据本发明的加密装置、加密程序、解密装置、解密程序、数据提供装置、数据接收装置及数据提供系统的第二实施方式。另外，该实施方式的数据提供装置、数据接收装置及数据提供系统是影像内容分发装置、影像内容接收装置及影像内容提供系统。

[0105] (B-1) 第二实施方式的构成

[0106] 图 11 是表示该实施方式的影像内容分发系统 1A 的整体构成的方框图。

[0107] 在第一实施方式中，设成，在影像内容分发装置 10 中，基于事先加密部 13 的加密和基于实时加密部 15 的加密所使用的加密条件（例如加密密钥的内容和加密方式等）相同而进行了说明。在第二实施方式中，下文所述的事先加密部 13A 和实时加密部 15A 的加密处理中加密条件不同。下面说明第二实施方式与第一实施方式的差异。

[0108] 影像内容分发系统 1A 具有影像内容分发装置 10A 及影像内容接收装置 20A。

[0109] 影像内容分发装置 10A 具有数据分割部 11、加密装置 12A 及数据分发部 16。数据分割部 11 和数据分发部 16 与第一实施方式相同，因此省略其说明。

[0110] 加密装置 12A 具有事先加密部 13A、数据积累部 14 及实时加密部 15A。数据积累部 14 与第一实施方式相同，因此省略其说明。

[0111] 图 12 是表示事先加密部 13A 的内部构成的方框图。

[0112] 事先加密部 13A 具有数据读入处理部 131、加密判定部 132A、加密处理部 133A 及加密标志设定部 134。数据读入处理部 131 与第一实施方式相同，因此省略其说明。

[0113] 加密判定部 132A 与第一实施方式的加密判定部 132 相同，在该实施方式中，作为例子，设成判定为每隔一个等规定间隔对 TS 数据包进行加密而进行说明。另外，与第一实施方式的加密判定部 132 相同，判定是否加密 TS 数据包的方法并不受此限定。

[0114] 加密处理部 133A 与第一实施方式的加密处理部 133 大致相同，但设定为与实时加密部 15A（下文所述的加密处理部 153A）相比，对 TS 数据包进行加密的条件不同。在加密处理部 133A 和下文所述的加密处理部 153A 中，例如可使用不同的加密密钥进行加密，甚至也可改变加密的方式。

[0115] 加密标志设定部 134，对加密处理部 133A 提供的 TS 数据包的头信息（例如加密标志）赋予表示由事先加密部 13 已加密这一情况的信息，并且提供给数据积累部 14。加密标志设定部 134 对 TS 数据包的加密标志设定与加密处理部 133 加密的 TS 数据包不同的值。在该实施方式中，作为例子，当在数据分割部 11 中生成了 TS 数据包的情况下，将加密标志的初始值设为“00”，对事先加密部 13A（加密标志设定部 134）设定为“01”，对实时加密部 15A（下文所述的加密标志设定部 154A）设定为“10”。据此，在影像内容接收装置 20A 中，识别是利用事先加密部 13A 的加密条件而加密的 TS 数据包，还是利用实时加密部 15A 的加密条件而加密的 TS 数据包。

[0116] 图 13 是表示实时加密部 15A 的内部构成的方框图。

[0117] 实时加密部 15A 具有数据读入处理部 151、加密判定部 152、加密处理部 153A 和加密标志设定部 154A。数据读入处理部 151 和加密判定部 152 与第一实施方式相同，因此省略其说明。

[0118] 加密处理部 153A 与第一实施方式的加密处理部 153 大致相同，但如上所述，设定为与事先加密部 13A（加密处理部 133A）相比，对 TS 数据包进行加密的条件不同。

[0119] 加密标志设定部 154A 与第一实施方式的加密标志设定部 154 大致相同，但如上所述，所设定的加密标志的内容与事先加密部 13A（加密标志设定部 134）不同。

[0120] 影像内容接收装置 20A 具有解密装置 21A 和输出部 22。

[0121] 输出部 22 与第一实施方式相同，因此省略其说明。

[0122] 图 14 是表示解密装置 21A 的内部构成的方框图。

[0123] 解密装置 21A 具有数据接收部 211、加密判定部 212 及解密处理部 213A。数据接收部 211 及加密判定部 212 与第一实施方式相同，因此省略其说明。

[0124] 解密处理部 213A 与第一实施方式的解密处理部 213 大致相同，但如上所述，由于有时每个 TS 数据包的加密条件不同，所以根据 TS 数据包的加密标志的内容，选择并适用对应于加密条件的解密条件，这一点与第一实施方式的解密处理部 213 不同。其他的功能与第一实施方式相同。

[0125] 如上所述，TS 数据包中的加密标志为“01”或“10”，因此解密处理部 213A 保持利用与每个加密标志对应的解密条件进行解密所必需的加密密钥的信息等。关于解密所必需的信息等，可以预先登记，也可以每次接收数据时从影像内容分发装置 10A 或省略图示的外部认证装置等读入并保持，对其取得方法不作限定。

[0126] (B-2) 第二实施方式的动作

[0127] 接着，说明具有上述构成的第二实施方式的影像内容分发系统 1A 的动作。

[0128] 如上所述，在第二实施方式的影像内容分发装置 10A 中，在事先加密部 13A 和实时加密部 15A 中 TS 数据包的加密所使用的加密条件不同，并且，在解密处理部 213A 中对此进行识别并解密，这点与第一实施方式存在差异。

[0129] 图 15 是表示在影像内容分发系统 1A 中将影像内容数据 30 从影像内容分发装置 10A 向影像内容接收装置 20A 分发的动作的整体的流程图。另外，步骤 S210、S230、S250 分别与上述步骤 S110、S130、S150（参照图 7）相同，因此省略其说明。

[0130] 在步骤 S220 和 S240 中，每个步骤进行的加密所适用的加密条件不同，除此之外与上述的步骤 S120 和步骤 S140（参照图 7）大致相同，因此省略详细的说明。

[0131] 在步骤 S260 中，解密装置 21A 中若被提供了 TS 数据包，则根据加密标志的内容选择适用的解密条件，并对该 TS 数据包进行解密，这一点与上述的步骤 S150（参照图 7）不同，除此之外的构成大致相同，因此省略详细的说明。

[0132] 接着，说明上述步骤 S220 中的事先加密部 13A 的动作的详细情况。

[0133] 图 16 是表示事先加密部 13A 的动作的详细情况的流程图。

[0134] 步骤 S221 ～ S223 的动作与上述步骤 S121 ～ S123 相同，因此省略其说明。

[0135] 而且，若将 TS 数据包从加密判定部 132A 提供给加密处理部 133A，则由加密处理部 133A 利用与实时加密部 15A（加密处理部 153A）不同的条件对该 TS 数据包进行加密，并提供给加密标志设定部 134(S224)。

[0136] 而且，若从加密处理部 133A 提供了 TS 数据包，则在加密标志设定部 134 中，对该 TS 数据包的加密标志设定“01”，并将设定了加密标志的 TS 数据包提供给数据积累部 14(S225、S226)。

[0137] 接着，说明上述步骤 S240 中的实时加密部 15A 的动作的详细情况。

[0138] 图 17 是表示上述步骤 S240 中的实时加密部 15A 的动作的详细情况的流程图。

[0139] 步骤 S241 ～ S243 的动作与上述步骤 S141 ～ S143 相同，因此省略其说明。

[0140] 而且，若将 TS 数据包从加密判定部 152 提供给了加密处理部 153A，则由加密处理部 153A 利用与事先加密部 13A（加密处理部 133A）不同的条件对该 TS 数据包进行加密，并提供给加密标志设定部 154A(S244)。

[0141] 若从加密处理部 153A 提供了 TS 数据包，则在加密标志设定部 154A 中，对该 TS 数

据包的加密标志设定“10”，并将设定了加密标志的 TS 数据包提供给数据分发部 16 进行分发 (S245、S246)。

[0142] 图 18 是表示上述步骤 S260 中的解密装置 21A 的动作的详细情况的流程图。

[0143] 步骤 S261 ～ S263 的动作与上述步骤 S161 ～ S163 相同，因此省略其说明。

[0144] 而且，若从加密判定部 212 提供了 TS 数据包，则在解密处理部 213A 中，适用与该 TS 数据包的加密标志对应的加密条件，进行解密，并提供给输出部 22(S264、S265)。

[0145] (B-3) 第二实施方式的效果

[0146] 根据该实施方式，除了第一实施方式的效果以外，还可取得以下效果。

[0147] 事先加密部 13A 和实时加密部 15A 中适用不同的加密密钥等加密条件，因此与第一实施方式相比提高了安全强度。例如，即使在非法取得了事先加密部 13A 的解密密钥时，由于无法解密由实时加密部 15A 加密的 TS 数据包，所以能够防止容易地重放（阅览）影像内容数据 30 的情况。

[0148] (C) 其他实施方式

[0149] 本发明并不限定于上述各实施方式，还可举出下面示例的变形实施方式。

[0150] (C-1) 在上述各实施方式中，解密装置具有加密判定部，根据 TS 数据包的加密标志的内容，判定该 TS 数据包是否已加密，并仅将已被加密的 TS 数据包提供给解密处理部进行解密，但也可以不设置加密判定部，将接收到的 TS 数据包全部设为已被加密而进行解密。

[0151] (C-2) 在第一实施方式中，事先加密部 13 中未设置加密标志设定部，但也可与第二实施方式的事先加密部 13A 同样设置加密标志设定部 134，对由事先加密部 13（加密处理部 133) 加密的 TS 数据包设定加密标志。

[0152] 例如，与第二实施方式相同，可以在数据分割部 11 中最初生成 TS 数据包时，将加密标志的初始值全部设定为“00”，对事先加密部 13 设定为“01”，对实时加密部 15 设定为“10”，在事先加密部 13 和实时加密部 15 中设定不同的加密标志。在此种情况下，影像内容接收装置 20 也能够在加密标志为“00”或“10”时判断为该 TS 数据包已被加密。

[0153] 此外，在第一实施方式中，可以仅在事先加密部 13 中设置加密标志设定部，在实时加密部 15 中不设置。在此种情况下，例如，在将数据分割部 11 中的加密标志的初始值设定为“00”，对事先加密部 13 设定为“01”的情况下，将加密标志为“01”的 TS 数据包判定为已经被加密，将加密标志为“00”的 TS 数据包判定为未被加密。此外，在解密装置 21 中，在已接收的全部 TS 数据包已被加密的情况下，即使是不由加密判定部 212 进行是否已加密的判定的构成，也能够正常地对 TS 数据包解密。

[0154] (C-3) 在上述各实施方式中，就影像内容分发装置 10 将影像内容数据分发至影像内容接收装置 20 的构成进行了说明，但分发对象的数据不限于影像内容，也可以是图像数据、语音数据、游戏软件、书籍数据等，进行分发的数据的对象并不限定于影像内容。分发对象的数据为影像内容之外的数据时，可至少将由分发对象数据分割而得到的数据和具有相当于上述加密标志的信息的数据作为一个单位，与 TS 数据包同样地加密并分发至数据接收装置。

[0155] (C-4) 在上述各实施方式中，作为加密标志，使用了 Transport_scrambling_control，但也可以使用其他头信息，还可以采用将净荷的开头数位用作加密标志等方式，

并不限定于 Transport_scrambling_control。

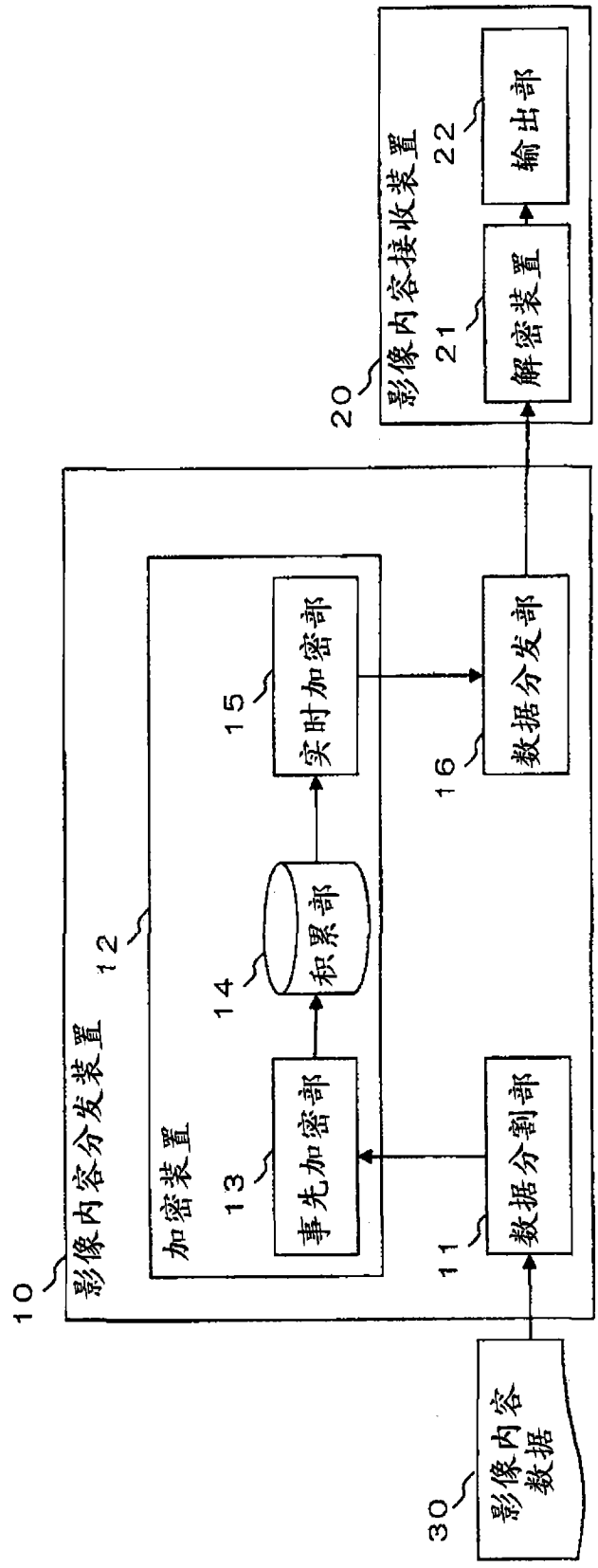

1 影像内容分发系统
影像内容分发装置
10
加密装置
12
事先加密部
13
积累部
14
实时加密部
15
数据分发部
16
数据分割部
11
影像内容数据
30
影像内容接收装置
20
解密装置
21
输出部
22

图1

名称	位数	说明
Sync_byte	8	固定为0x47
Transport_error_indicator	1	错误标志
Payload_unit_start_indicator	1	开始标志
Transport_priority	1	优先级
PID	13	净荷类别
Transport_scrambling_control	2	加密控制
Adaptation_control	2	附加信息控制
Continuity_counter	4	连续性计数
Adaptation_field	-	附加信息
Data_byte	-	净荷

图 2

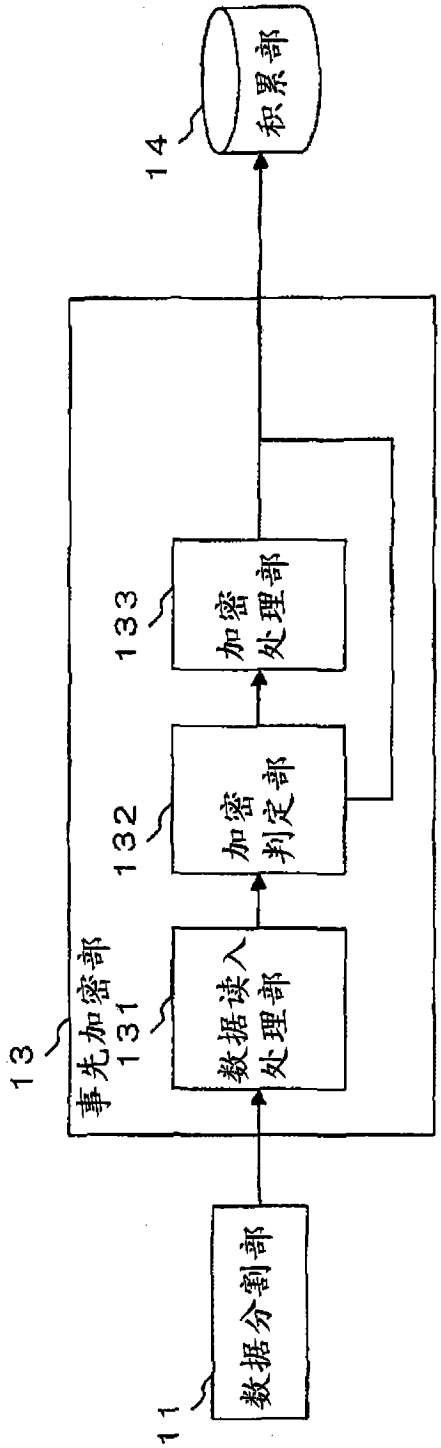


图 3

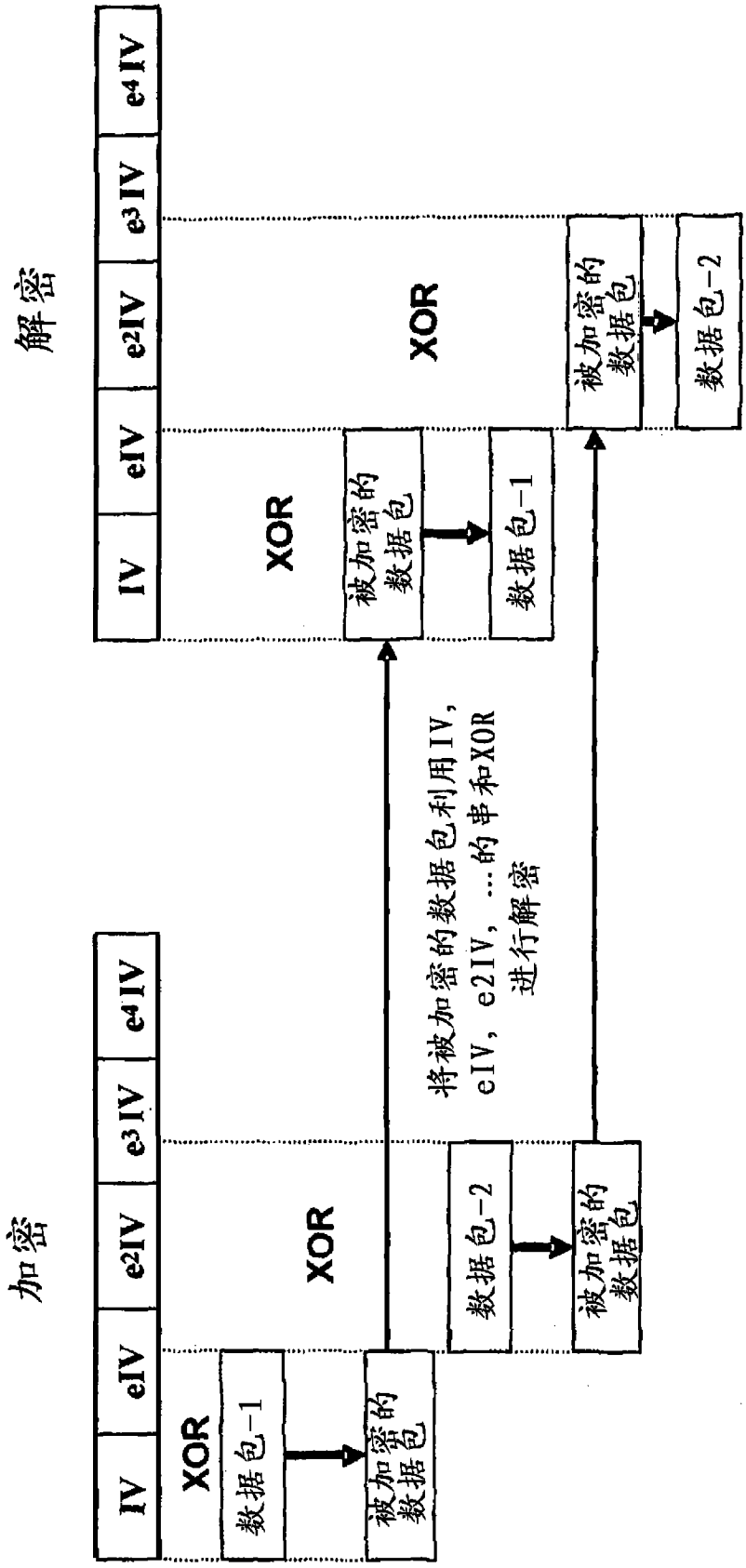

加密
IV
eIV
e2IV
e3IV
e4IV
XOR
数据包-1
被加密的数据包
数据包-2
被加密的数据包
将被加密的数据包利用IV，eIV，e2IV，...的串和XOR进行解密
解密
IV
eIV
e2IV
e3IV
e4IV
XOR
被加密的数据包
数据包-1
被加密的数据包
数据包-2

图 4

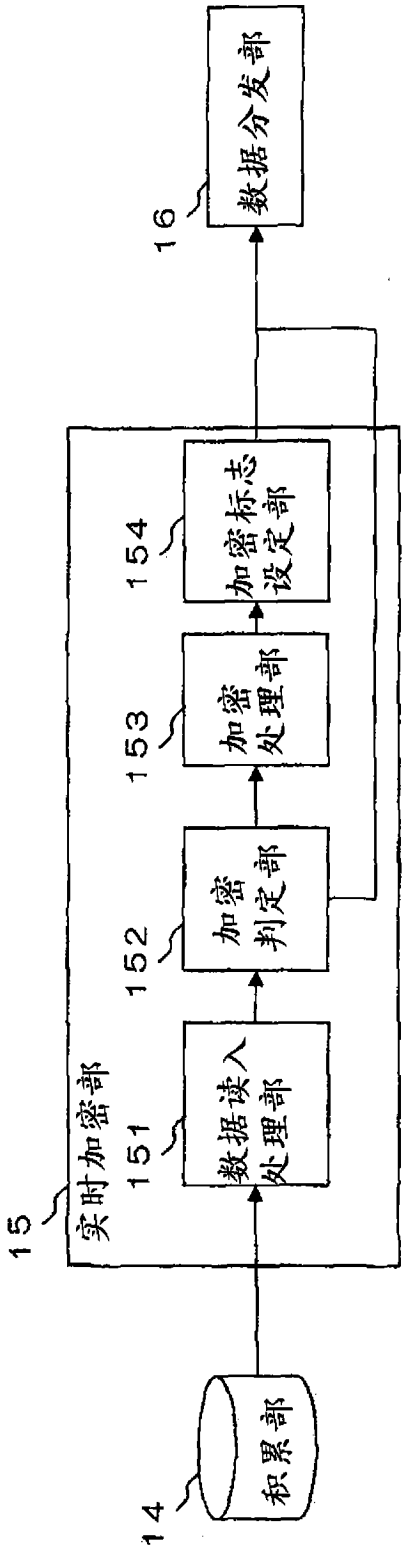

14
积累部
15
实时加密部
151
数据读入处理部
152
加密判定部
153
加密处理部
154
加密标志设定部
16
数据分发部

图 5

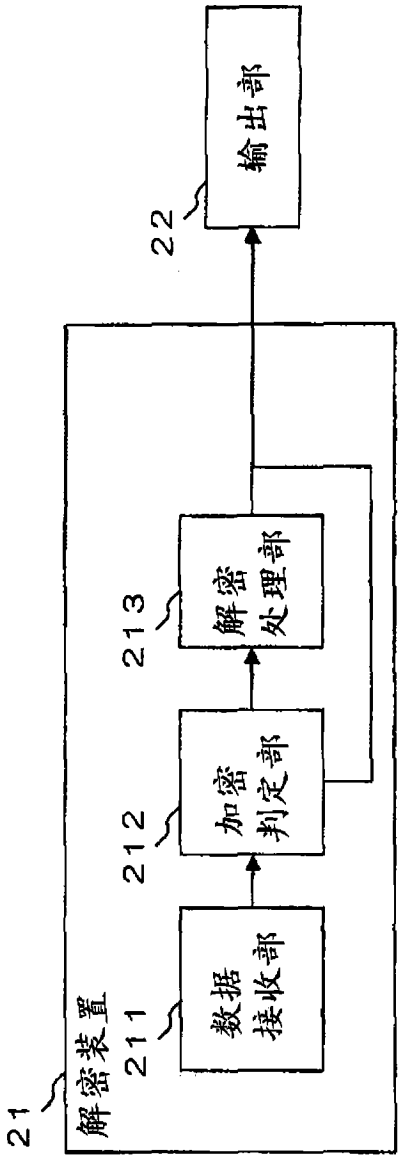

21
解密装置
211
数据接收部
212
加密判定部
213
解密处理部
22
输出部

图6

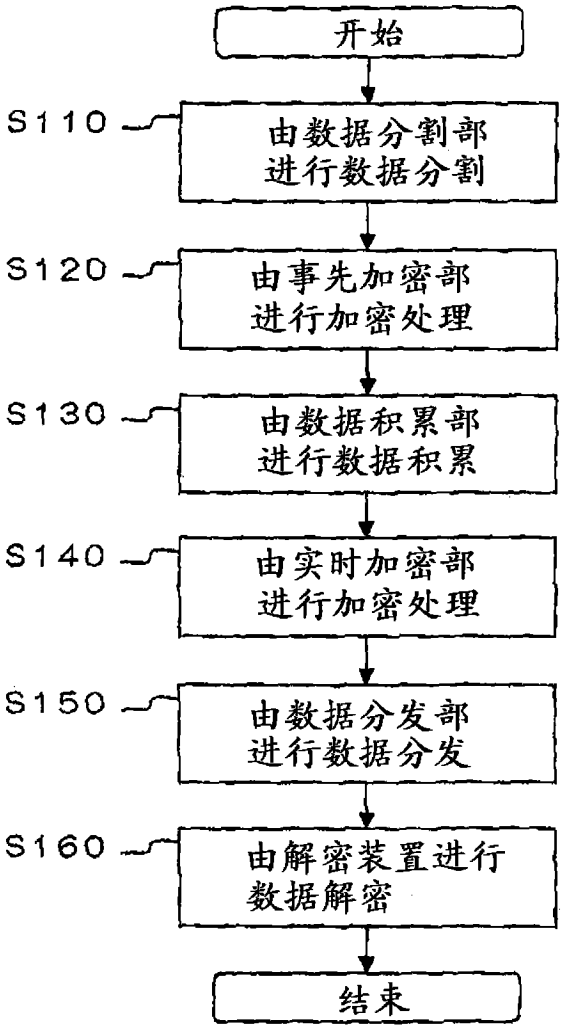

开始
S110
由数据分割部进行数据分割
S120
由事先加密部进行加密处理
S130
由数据积累部进行数据积累
S140
由实时加密部进行加密处理
S150
由数据分发部进行数据分发
S160
由解密装置进行数据解密
结束

图 7

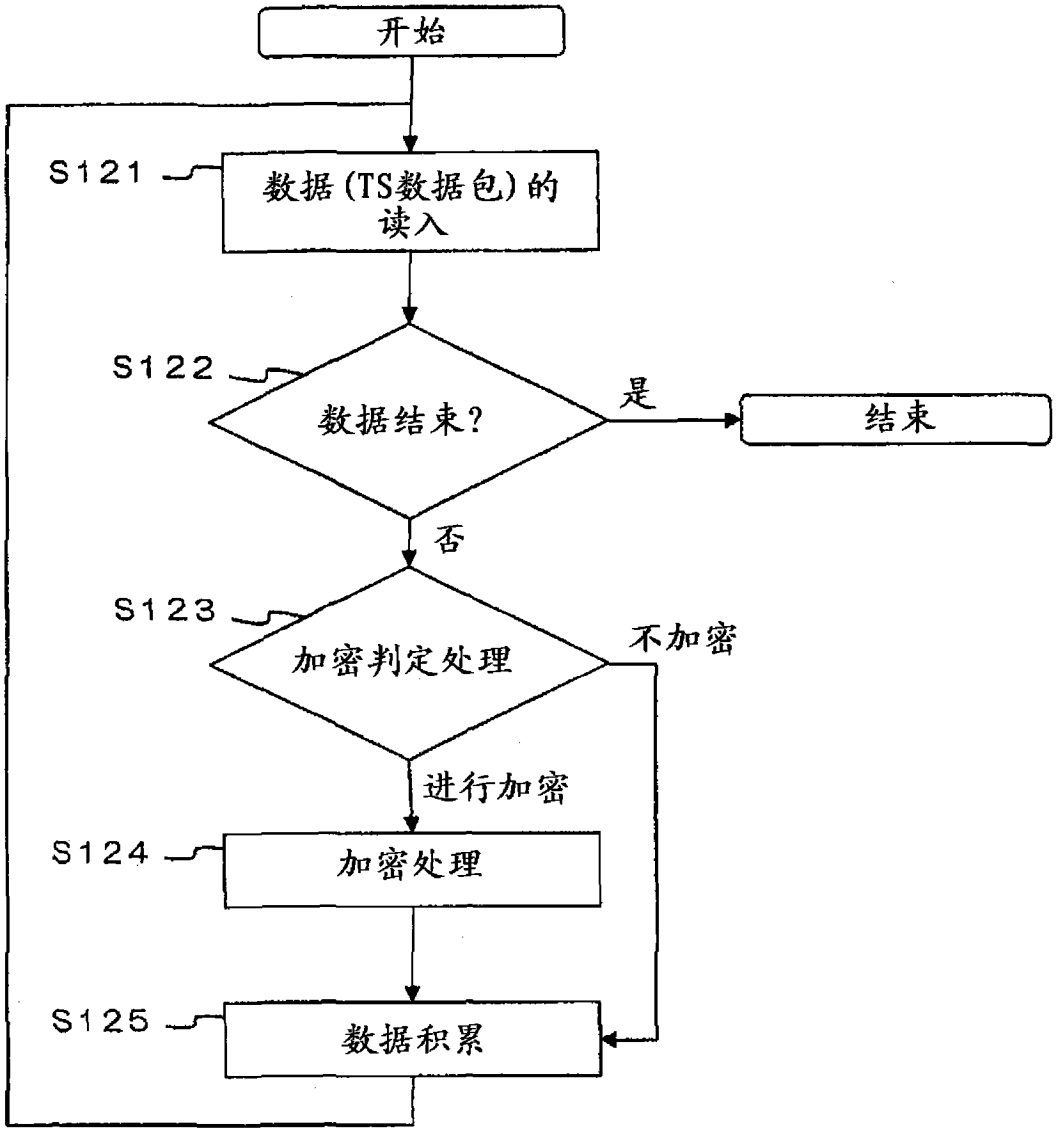

开始
S121
数据(TS数据包)的读入
S122
数据结束?
是
结束
否
S123
加密判定处理
不加密
进行加密
S124
加密处理
S125
数据积累

图 8

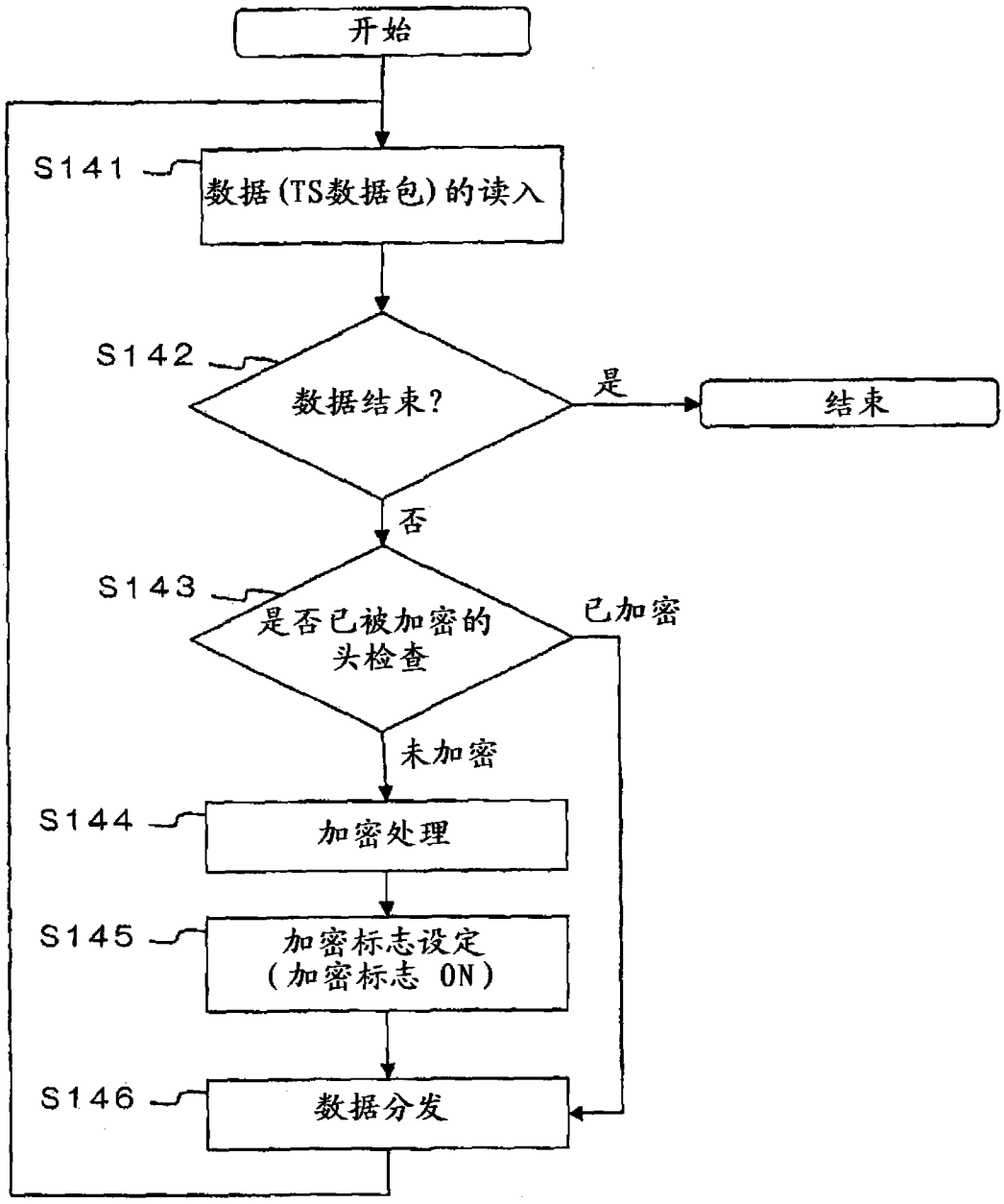

开始
S141
数据(TS数据包)的读入
S142
数据结束?
是
结束
否
S143
是否已被加密的
头检查
已加密
未加密
S144
加密处理
S145
加密标志设定
(加密标志 ON)
S146
数据分发

图 9

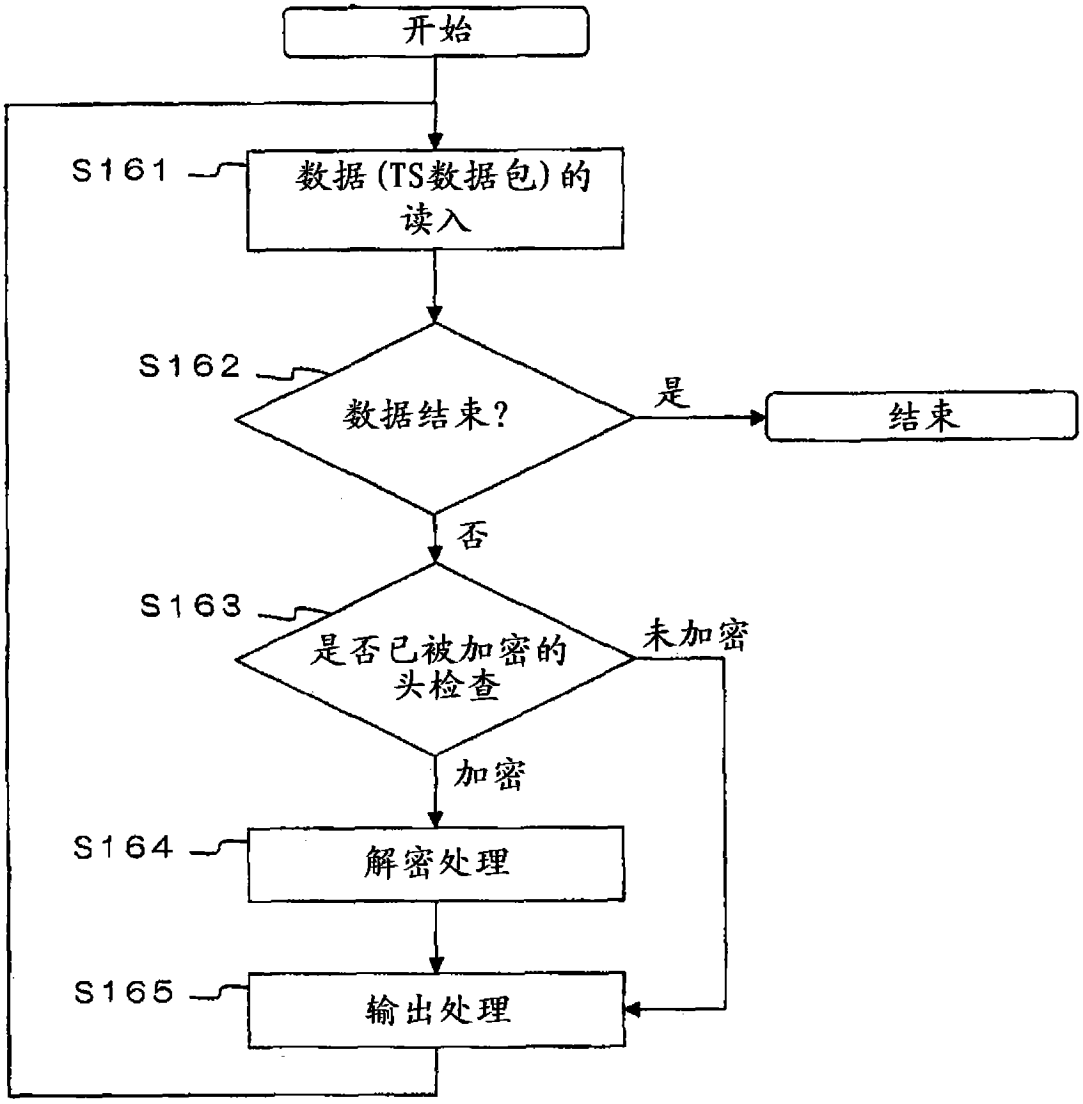

开始
S161
数据(TS数据包)的读入
S162
数据结束?
是
结束
否
S163
是否已被加密的头检查
未加密
加密
S164
解密处理
S165
输出处理

图 10

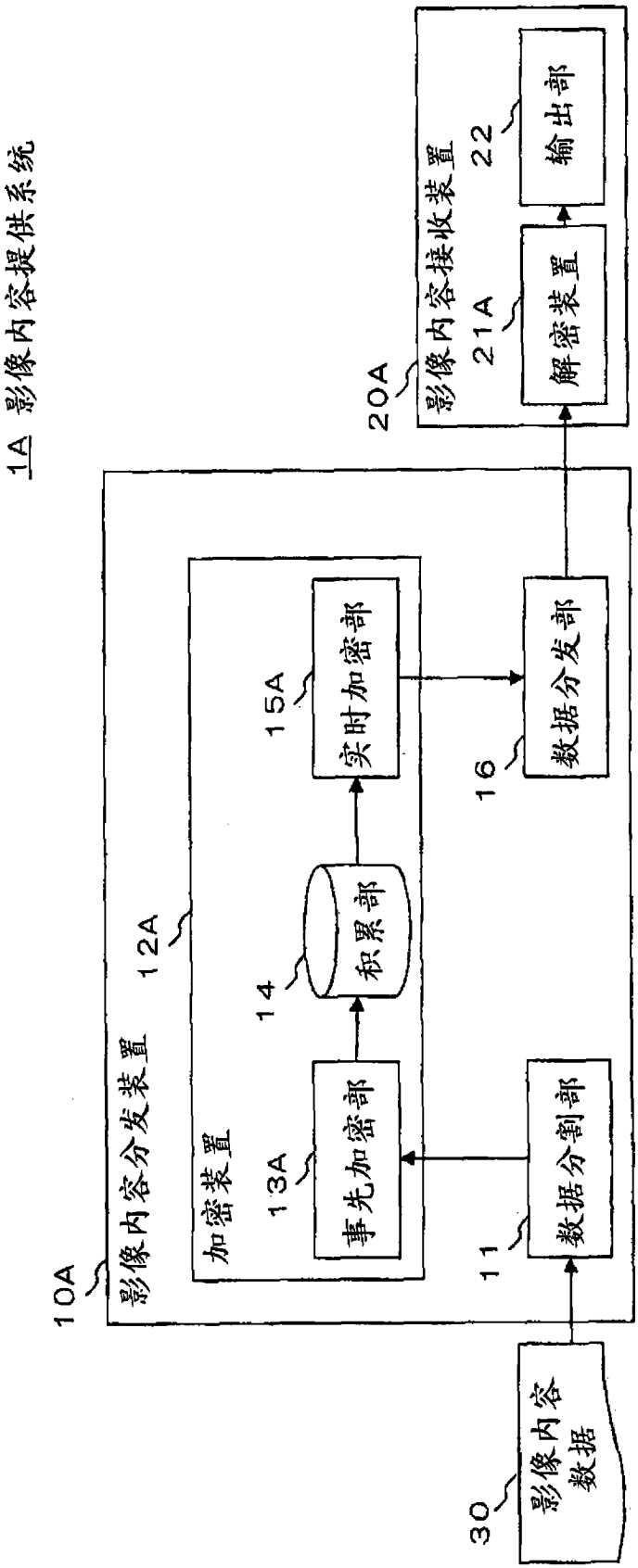

1A 影像内容提供系统
10A
影像内容分发装置
12A
加密装置
13A
事先加密部
14
积累部
15A
实时加密部
16
数据分发部
11
数据分割部
30
影像内容数据
20A
影像内容接收装置
21A
解密装置
22
输出部

图11

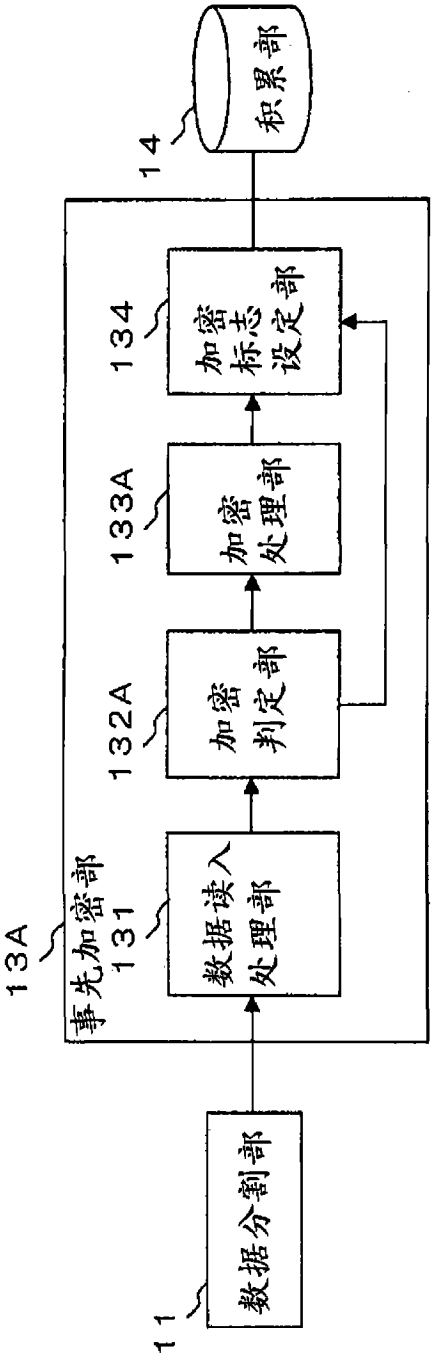

数据分割部
11
事先加密部
13A
数据读入处理部
131
加密判定部
132A
加密处理部
133A
加密标志设定部
134
积累部
14

图12

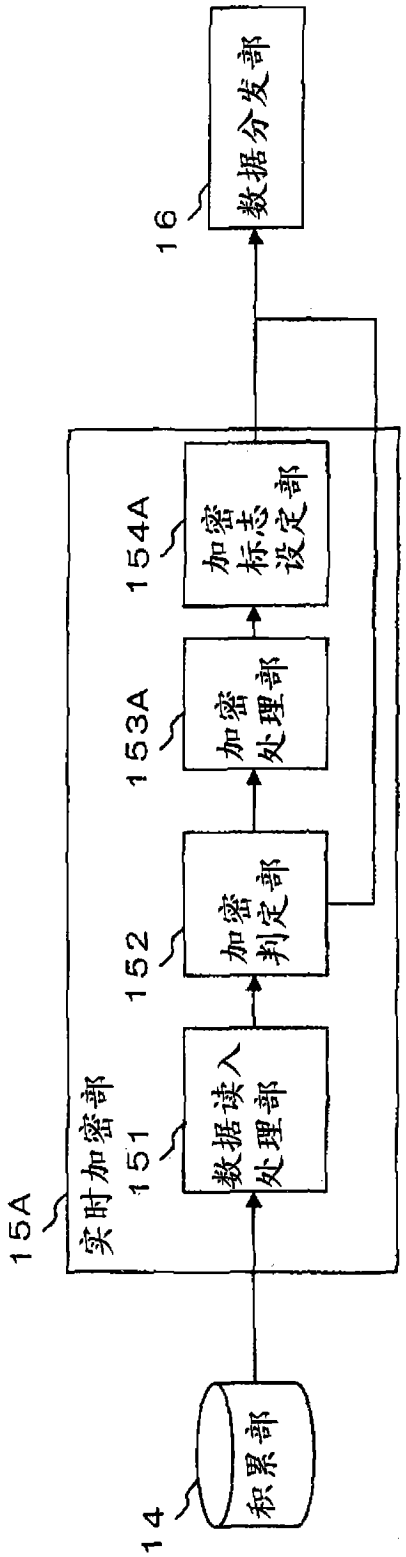

14
积累部
15A
实时加密部
151
数据读入处理部
152
加密判定部
153A
加密处理部
154A
加密标志设定部
16
数据分发部

图13

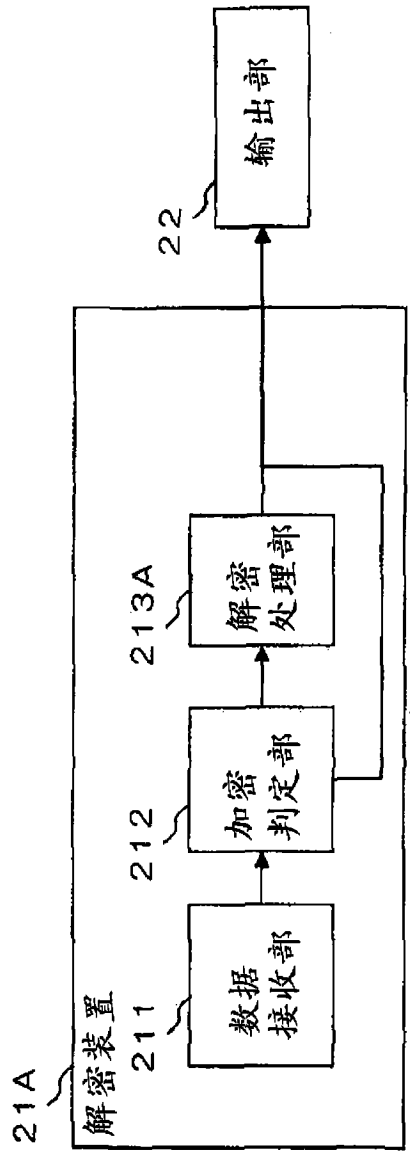


图14

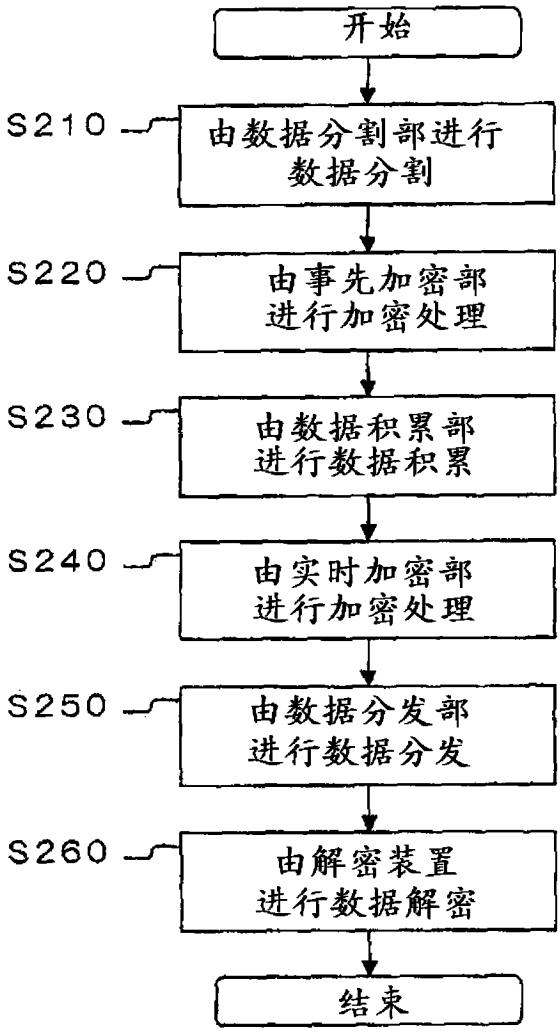

开始
S210
由数据分割部进行数据分割
S220
由事先加密部进行加密处理
S230
由数据积累部进行数据积累
S240
由实时加密部进行加密处理
S250
由数据分发部进行数据分发
S260
由解密装置进行数据解密
结束

图 15

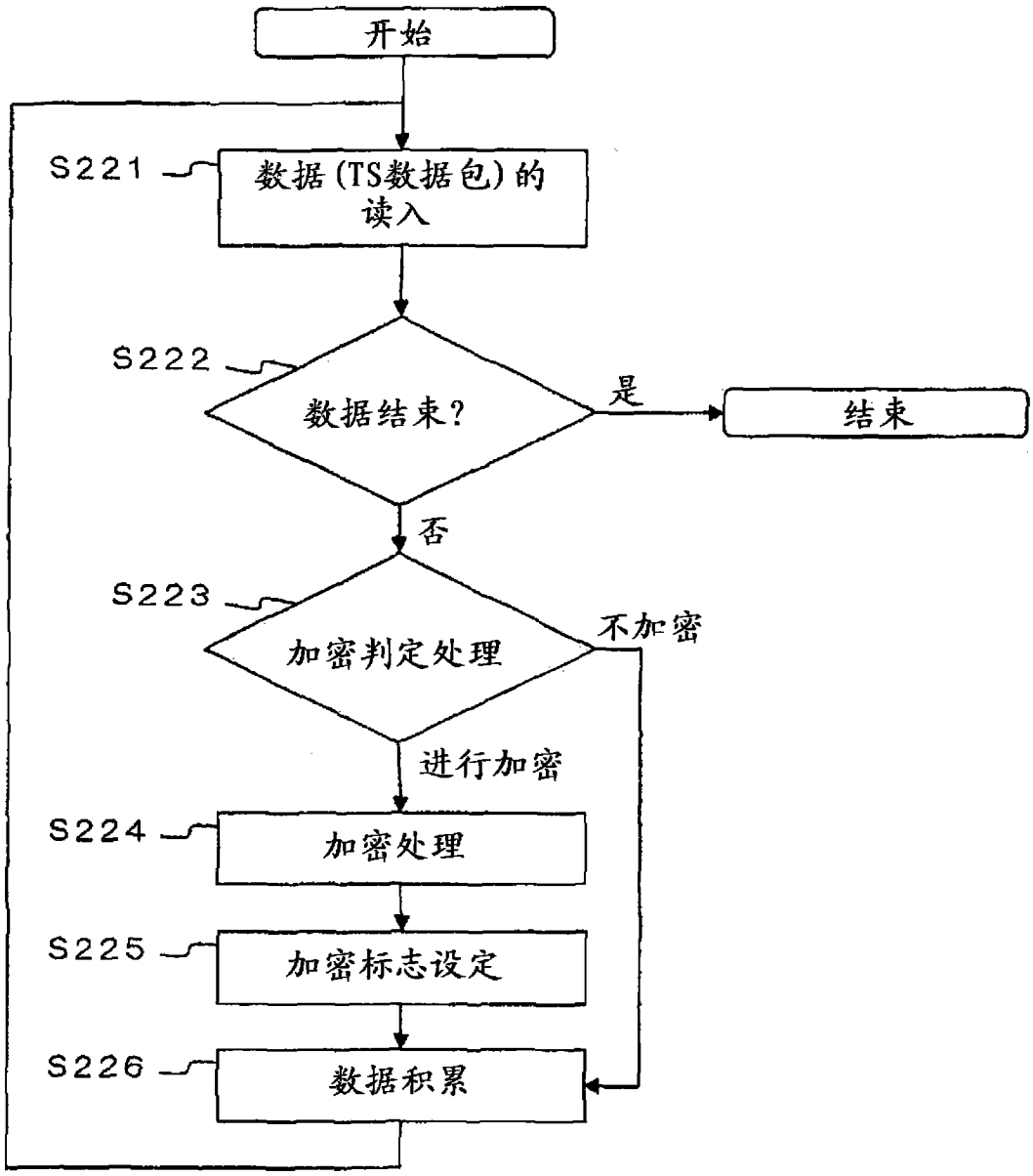

开始
S221
数据(TS数据包)的读入
S222
数据结束?
是
结束
否
S223
加密判定处理
不加密
进行加密
S224
加密处理
S225
加密标志设定
S226
数据积累

图 16

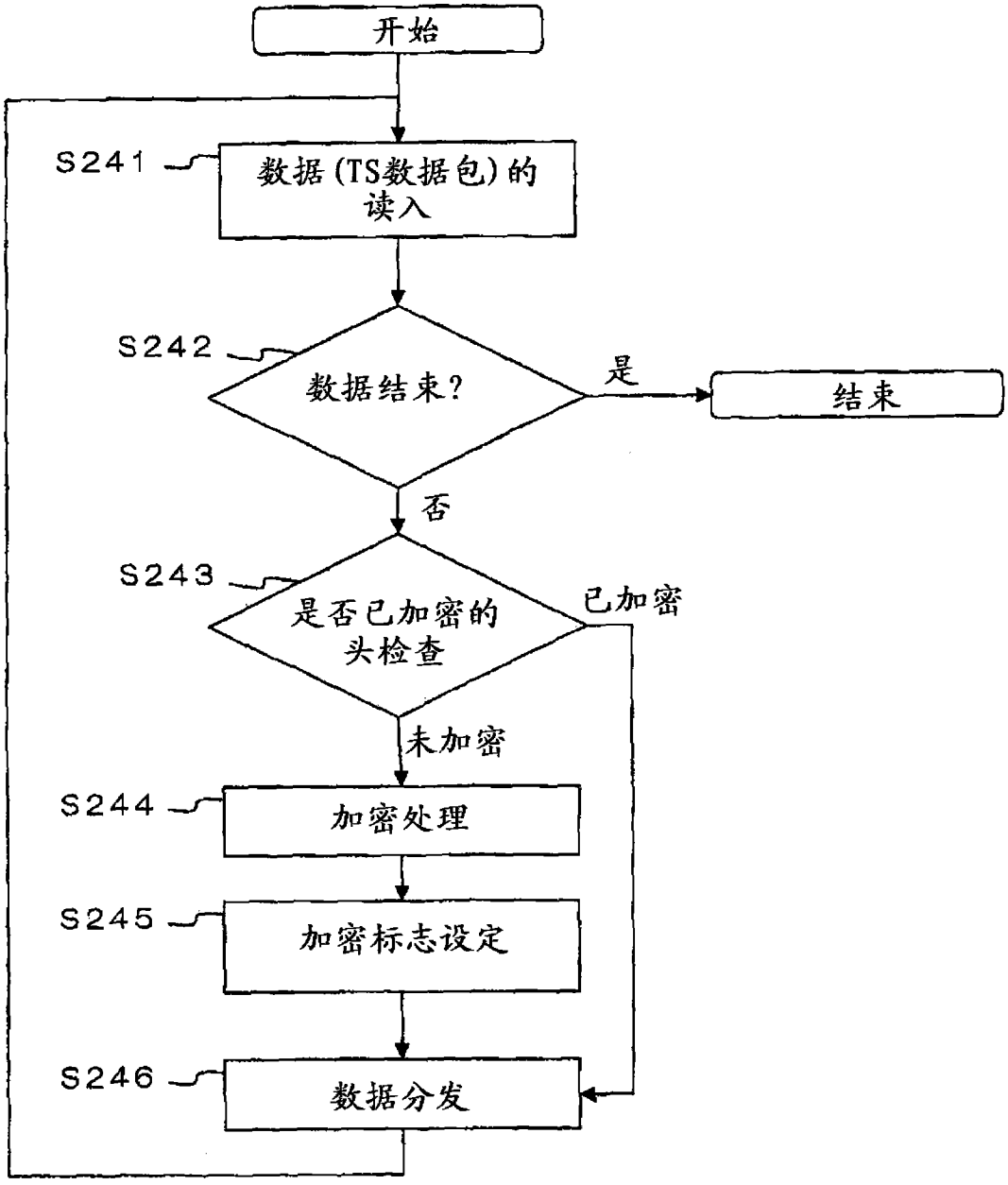

开始
S241
数据(TS数据包)的读入
S242
数据结束?
是
结束
否
S243
是否已加密的头检查
已加密
未加密
S244
加密处理
S245
加密标志设定
S246
数据分发

图 17

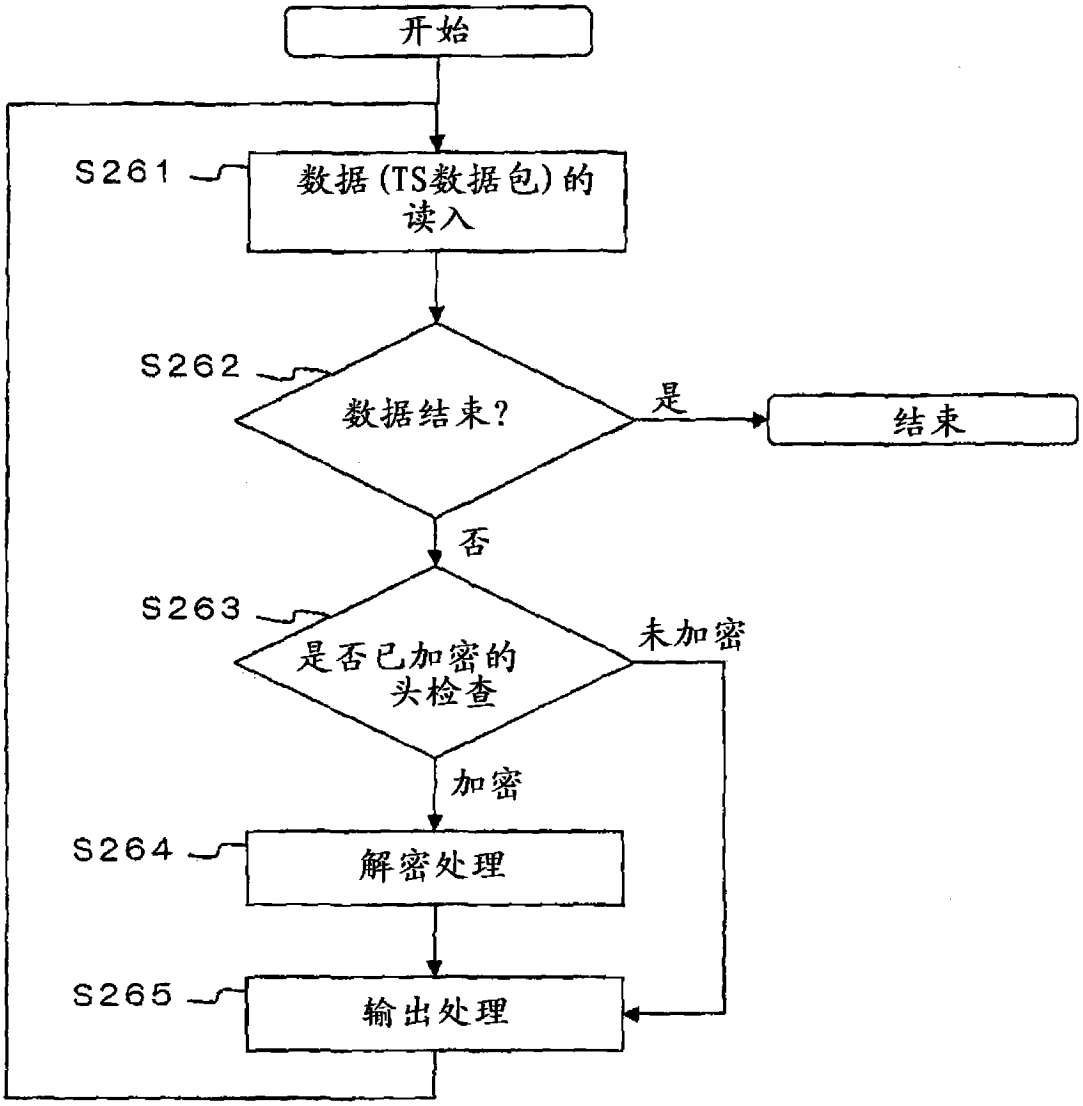

开始
S261
数据(TS数据包)的读入
S262
数据结束?
是
结束
否
S263
是否已加密的头检查
未加密
加密
S264
解密处理
S265
输出处理

图 18